

日 本 国 特 許 庁
JAPAN PATENT OFFICE

07. 2. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 2 月 9 日
Date of Application:

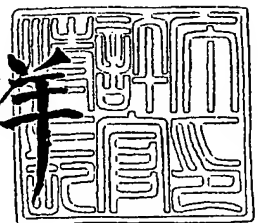
出 願 番 号 特 願 2 0 0 4 - 0 3 2 6 7 6
Application Number:
[ST. 10/C]: [J P 2 0 0 4 - 0 3 2 6 7 6]

出 願 人 松下電器産業株式会社
Applicant(s):

2 0 0 5 年 3 月 1 0 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋
BEST AVAILABLE COPY



【書類名】 特許願
【整理番号】 2048150058
【あて先】 特許庁長官殿
【国際特許分類】 G06F
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 中野 稔久
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 原田 俊治
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 山本 雅哉
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 岡本 隆一
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100109210
 【弁理士】
 【氏名又は名称】 新居 広守
【手数料の表示】
 【予納台帳番号】 049515
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 0213583

【書類名】 特許請求の範囲**【請求項 1】**

デジタルコンテンツの利用可能な範囲を示すライセンス情報を管理するライセンス情報管理装置であって、安全にデータ制御を行うデータ制御手段と安全にデータの記憶を可能とする記憶手段とを備え、

前記データ制御手段は、

秘密鍵を保持する秘密鍵保持部と、

前記秘密鍵でライセンス情報を暗号化する暗号化部と、

前記暗号化されたライセンス情報を前記記憶手段に移管する移管部とを備える

ことを特徴とするライセンス情報管理装置。

【請求項 2】

前記データ制御手段は、さらに、

前記記憶手段から暗号化されたライセンス情報を読み出す読出部と、

前記読み出されたライセンス情報を復号する復号部と、

デジタルコンテンツの利用に応じて前記復号されたライセンス情報を更新する情報更新部と、

前記更新されたライセンス情報を暗号化して、前記記憶手段に上書きする上書部とを備える

ことを特徴とする請求項 1 記載のライセンス情報管理装置。

【請求項 3】

前記記憶手段は、さらに、

前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表についてデジタル署名を施したデータを記憶する署名データ記憶部を備え、

前記データ制御手段は、さらに、

前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表を記憶する対応表記憶部と、

前記署名データ記憶部におけるデジタル署名を施したデータと、前記対応表とに基づいて、前記ライセンス情報の正当性を検証する情報検証部を備える

ことを特徴とする請求項 2 記載のライセンス情報管理装置。

【請求項 4】

前記更新履歴を表わす情報は、

アップデート回数又は乱数を表わす情報である

ことを特徴とする請求項 3 記載のライセンス情報管理装置。

【請求項 5】

前記デジタルコンテンツは暗号化されており、

前記ライセンス情報は、

前記デジタルコンテンツの利用可能な範囲を示す条件を規定する再生条件情報と前記デジタルコンテンツを復号するためのコンテンツ鍵とを含む

ことを特徴とする請求項 1～4 記載のライセンス情報管理装置。

【請求項 6】

デジタルコンテンツの利用可能な範囲を示すライセンス情報を管理するライセンス情報管理方法であって、

前記ライセンス情報管理方法は、

安全にデータ制御を行うデータ制御ステップを有し、

前記データ制御ステップは、

秘密鍵を保持する秘密鍵保持サブステップと、

前記秘密鍵でライセンス情報を暗号化する暗号化サブステップと、

前記暗号化されたライセンス情報を安全にデータの記憶を可能とする記憶手段に移管する移管サブステップとを含む

ことを特徴とするライセンス情報管理方法。

【請求項 7】

前記データ制御ステップは、さらに、
前記記憶手段から暗号化されたライセンス情報を読み出す読出サブステップと、
前記読み出されたライセンス情報を復号する復号サブステップと、
デジタルコンテンツの利用に応じて前記復号されたライセンス情報を更新する情報更新サブステップと、
前記更新されたライセンス情報を暗号化して、前記記憶手段に上書きする上書サブステップとを含む
ことを特徴とする請求項 6 記載のライセンス情報管理方法。

【請求項 8】

前記記憶手段は、さらに、
前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表についてデジタル署名を施したデータを記憶する署名データ記憶部と、前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表を記憶する対応表記憶部とを備え、
前記データ制御ステップは、さらに、
前記署名データ記憶部におけるデジタル署名を施したデータと、前記対応表とに基づいて、前記ライセンス情報の正当性を検証する情報検証サブステップを含む
ことを特徴とする請求項 7 記載のライセンス情報管理方法。

【請求項 9】

デジタルコンテンツの利用可能な範囲を示すライセンス情報を管理するライセンス情報管理装置のためのプログラムであって、
前記プログラムは、
安全にデータ制御を行うデータ制御ステップを有し、
前記データ制御ステップは、
秘密鍵を保持する秘密鍵保持サブステップと、
前記秘密鍵でライセンス情報を暗号化する暗号化サブステップと、
前記暗号化されたライセンス情報を安全にデータの記憶を可能とする記憶手段に移管する移管サブステップとを
コンピュータに実行させることを特徴とするプログラム。

【請求項 10】

前記データ制御ステップは、さらに、
前記記憶手段から暗号化されたライセンス情報を読み出す読出サブステップと、
前記読み出されたライセンス情報を復号する復号サブステップと、
デジタルコンテンツの利用に応じて前記復号されたライセンス情報を更新する情報更新サブステップと、
前記更新されたライセンス情報を暗号化して 前記記憶手段に上書きする上書サブステップとを含む
ことを特徴とする請求項 9 記載のプログラム。

【請求項 11】

前記記憶手段は、さらに、
前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表についてデジタル署名を施したデータを記憶する署名データ記憶部と、前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表を記憶する対応表記憶部とを備え、
前記データ制御ステップは、さらに、
前記署名データ記憶部におけるデジタル署名を施したデータと、前記対応表とに基づいて、前記ライセンス情報の正当性を検証する情報検証サブステップを含む
ことを特徴とする請求項 10 記載のプログラム。

【書類名】 明細書

【発明の名称】 ライセンス情報管理装置およびライセンス情報管理方法

【技術分野】

【0001】

本発明は、暗号化されているデジタルコンテンツ等を再生する際の鍵情報や再生条件などを規定したライセンス情報の管理装置及びその管理方法に関し、特に、耐タンパ性を確保しながら上記ライセンス情報を管理する技術に関する。

【背景技術】

【0002】

近年、ブロードバンド等のネットワークを利用したコンテンツ（例えば、映像、音声、プログラムソフトなど）配信が普及している。さらに、BD-ROM(Blue ray Disc-Read Only Memory)パッケージを用いたコンテンツ配信の検討も進んでいる。一般に、これらのコンテンツには暗号化が施されているため、ユーザは、コンテンツに対応する復号鍵を入手する必要がある。さらに、上記コンテンツは、料金の支払いを前提とした利用制限が課されている場合が多く、ユーザは、所定のライセンス情報（例えば、ライセンスチケット）に従ってコンテンツを利用することとなる。ここで、「ライセンスチケット」とは、コンテンツの利用を制限するための条件を規定した情報である「コンテンツ再生条件情報」と、受信したコンテンツを復号するための鍵である、暗号化されている「コンテンツ鍵」とを含む情報をいう。この「コンテンツ再生条件情報」は、例えば、再生可能な日時について規定したり、再生可能な総時間について規定したり、再生可能な回数について規定したりするための情報である。

【0003】

このため、ライセンスチケットについては厳重な管理が要求され、一般に、ライセンスチケットは、許可が認められないと書換えができない領域（耐タンパ領域）に保持される（例えば、特許文献1参照）。

図9は、従来の技術に係るコンテンツ再生装置500の機能構成を示すブロック図である。コンテンツ再生装置500は、暗号化されたコンテンツ（例えば、BSデジタル放送の場合であれば、コンテンツの暗号化には、スクランブル鍵、ワーク鍵及びマスタ鍵が使用される。）を再生（利用）する際に必要となるライセンスチケットを耐タンパ性を確保しながら管理する装置であり、耐タンパモジュール部（以下「TRM(Tamper Resistance Module)部」と記す。）510、コンテンツ復号部520、デコード部530及び操作入力部535を備える。なお、コンテンツ再生装置500は、他に外部のネットワークに接続してデータの送受信を制御する通信制御部等を備えてもよい。

【0004】

TRM部510は、例えば耐タンパ性を有するICカードで構成され、上記ライセンスチケットの管理を行う部署であり、コンテンツ再生条件情報511aと暗号化されたコンテンツ鍵511bを格納するライセンスチケット格納部511、コンテンツ再生条件情報511aに基づいてコンテンツの再生を制御するコンテンツ再生条件管理部512、TRM部510で使用する固有鍵等を格納するTRM固有鍵格納部513、及びTRM固有鍵を用いてコンテンツ鍵の復号を行うコンテンツ鍵復号部514を備える。

【0005】

コンテンツ復号部520は、コンテンツ鍵復号部514において復号されたコンテンツ鍵を用いて暗号化されたコンテンツ550の復号を行う。

デコード部530は、コンテンツ復号部520において復号されたコンテンツをディスプレイ540が表示可能なデータにデコードする。操作入力部535は、例えばスイッチやリモコン等であり、ユーザから「再生」などの操作を受け付けて、コンテンツ復号部520やコンテンツ再生条件管理部512に通知する。

【0006】

コンテンツ再生装置500の動作は、以下の通りである。

最初に、センタ600から入手されたTRM部510（ICカード）がコンテンツ再生

装置 500 のカード挿入口等 (図示せず) に挿入され、操作入力部 535 を介してユーザから再生指示を受け付けると、コンテンツ再生条件管理部 512 は、再生指示の対象となったコンテンツを特定し、ライセンスチケット格納部 511 から、上記コンテンツに対応するライセンスチケットのコンテンツ再生条件情報 511a を特定して、その内容を解読する。さらに、コンテンツ再生条件管理部 512 は、コンテンツ再生条件情報 511a の内容がコンテンツの再生を許可し得る条件であるか否かを判定し、再生が可能な場合は、ライセンスチケット格納部 511 に格納されている暗号化されたコンテンツ鍵 511b を読み出してコンテンツ鍵復号部 514 に送信する。コンテンツ鍵復号部 514 は、TRM 固有鍵格納部 513 から TRM 固有鍵を読み出し、暗号化されたコンテンツ鍵 511b を復号し、これをコンテンツ復号部 520 に送信する。コンテンツ復号部 520 は、コンテンツ鍵復号部 514 から受信した、復号されたコンテンツ鍵に基づいて上記コンテンツを復号し、復号したコンテンツをデコード部 530 に送信する。

【0007】

さらに、コンテンツ復号部 520 は、コンテンツの再生に関する情報 (例えば、コンテンツ名、再生開始日時、再生終了日時など) をコンテンツ再生条件管理部 512 に送信する。これにより、コンテンツ再生条件管理部 512 は、再生されたコンテンツに対応するコンテンツ再生条件情報 511a の内容を変更し、ライセンスチケット格納部 511 に上書きする。なお、上記のコンテンツ鍵復号部 514 とコンテンツ復号部 520 間は、SAC (Secure Authentication Channel: 認証付きの安全な通信路) で結ばれている。

【0008】

以上のように、コンテンツ再生装置 500 は、再生条件情報であるライセンスチケットを耐タンパ性を確保しながら管理している。

【特許文献 1】特開平 01-194029 号公報

【発明の開示】

【発明が解決しようとする課題】

【0009】

しかしながら、上記ライセンスチケットについては、利用料配分などを容易にするために「1 コンテンツ 1 ライセンスチケット」という形態をとっており、1 ユーザが多数のコンテンツを所有する場合は、これに応じてライセンスチケットの数も多くなり、ライセンスチケットを格納するためのメモリ容量も増大する。このため、大容量の TRM 部が必要となり、コンテンツ再生装置のコスト増につながり、最終的には競争力の低下の原因となる。

【0010】

そこで、本発明は、ユーザが多数のコンテンツを所有する場合であっても、大容量の TRM 部が必要とならないライセンス情報管理装置及びライセンス情報管理方法を提供することを目的とする。

【課題を解決するための手段】

【0011】

上記の目的を達成するために、本発明に係るライセンス情報管理装置は、デジタルコンテンツの利用可能な範囲を示すライセンス情報を管理するライセンス情報管理装置であって、安全にデータ制御を行うデータ制御手段と安全にデータの記憶を可能とする記憶手段とを備え、前記データ制御手段は、秘密鍵を保持する秘密鍵保持部と、前記秘密鍵でライセンス情報を暗号化する暗号化部と、前記暗号化されたライセンス情報を前記記憶手段に移管する移管部とを備える。

【0012】

これにより、従来 TRM 部 (耐タンパ性を有する IC カード) に格納していたライセンスチケットをセキュアフラッシュ部に格納することとしたので、TRM 部における記憶容量を最小限に抑えることが可能となる。

また、本発明に係るライセンス情報管理装置の前記データ制御手段は、さらに、前記記憶手段から暗号化されたライセンス情報を読み出す読出部と、前記読み出されたライセン

ス情報を復号する復号部と、デジタルコンテンツの利用に応じて前記復号されたライセンス情報を更新する情報更新部と、前記更新されたライセンス情報を暗号化して、前記記憶手段に上書きする上書部とを備えてもよい。

【0013】

さらに、本発明に係るライセンス情報管理装置の前記記憶手段は、さらに、前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表についてデジタル署名を施したデータを記憶する署名データ記憶部を備え、前記データ制御手段は、さらに、前記ライセンス情報を識別し得る識別情報と当該ライセンス情報の更新履歴を表す情報とを対応付けた対応表を記憶する対応表記憶部と、前記署名データ記憶部におけるデジタル署名を施したデータと、前記対応表とに基づいて、前記ライセンス情報の正当性を検証する情報検証部を備えるように構成することもできる。

【0014】

これにより、ライセンスチケットをセキュアフラッシュ部に格納すると共に、ライセンスチケットを識別し得る情報(LT_ID)とアップデート回数とが対応付けられている対応表に基づいてライセンスチケットの正当性も検証するので、TRM部の記憶容量を最小限に抑えたと共に、より安全性を高めてライセンスチケットを管理することが可能となる。

【0015】

なお、本発明は、上記ライセンス情報管理装置における特徴的な構成手段をステップとするライセンス情報管理方法として実現したり、それらステップをパーソナルコンピュータ等を実行させるプログラムとして実現したりすることもできる。そして、そのプログラムをDVD等の記録媒体やインターネット等の伝送媒体を介して広く流通させることができるのは言うまでもない。

【発明の効果】

【0016】

以上の説明から明らかなように、本発明によれば、従来TRM部(耐タンパ性を有するICカード)に格納していたライセンスチケットをセキュアフラッシュ部に格納することとしたので、TRM部における記憶容量を最小限に抑えることが可能となる。

さらに、本発明によれば、ライセンスチケットをセキュアフラッシュ部に格納すると共に、ライセンスチケットを識別し得る情報(LT_ID)とアップデート回数とが対応付けられている対応表に基づいてライセンスチケットの正当性も検証するので、TRM部の記憶容量を最小限に抑えたと共に、より安全性を高めてライセンスチケットを管理することが可能となる。

【0017】

従って、デジタル放送やパッケージソフト、ネットワーク等を介してデジタル著作物の流通や配信等が活発になり、適切な著作権保護の要請が高い今日においては、本願発明の実用価値は極めて高い。

【発明を実施するための最良の形態】

【0018】

以下、本発明に係る実施の形態について、図面を参照しながら詳細に説明する。
(実施の形態1)

図1は、本実施の形態に係るコンテンツ再生装置100の機能構成を示すブロック図である。図1のコンテンツ再生装置100は、暗号化されたコンテンツを再生(利用)する際に必要となるライセンスチケット(以下において、「LT(License Ticket)」とも記す。)を耐タンパ性を確保しながら管理する装置であり、TRM部110、セキュアフラッシュ部120、コンテンツ復号部520、デコード部530及び操作入力部535を備える。なお、コンテンツ再生装置100は、他に外部のネットワークに接続してデータの送受信を制御する通信制御部(図示せず)等を備えてもよい。

【0019】

なお、本コンテンツ再生装置100においては、上記従来技術のコンテンツ再生装置500と同一の機能構成については同一の符番を付し、その説明は省略することとする。

TRM部110は、例えば、耐タンパ性を有するICカードであり、コンテンツ再生条件管理部111、TRM固有鍵格納部513及びコンテンツ鍵復号部514を備える。

コンテンツ再生条件管理部111は、TRM部110全体の制御を行う部署であり、センタ600を介して入手した、暗号化されたコンテンツ550に対応するライセンスチケットを暗号化してセキュアフラッシュ部120に格納すると共に、ユーザによってコンテンツが再生される毎に、そのコンテンツに対応するコンテンツ再生条件情報511aの更新を行う部署である。

【0020】

セキュアフラッシュ部120は、例えば汎用のフラッシュメモリであるが、暗号化されたコンテンツ550に対応するライセンスチケット（即ち、コンテンツ再生条件情報511a及び暗号化されたコンテンツ鍵511b）の書き込み／読み出しの際には、TRM固有鍵によって暗号化／復号化が行われるという特徴を有している。具体的には、コンテンツ再生条件管理部111が、TRM固有鍵格納部513に格納されているTRM固有鍵を用いて、セキュアフラッシュ部120から読み出されたライセンスチケットの復号を行う。また、TRM固有鍵を用いて、更新されたライセンスチケットを暗号化し、これをセキュアフラッシュ部120に書き込む。

【0021】

図2は、上記コンテンツ再生条件管理部111の機能構成を示すブロック図である。図2に示されるように、コンテンツ再生条件管理部111は、再生状況分析部112、全体制御部113及び暗号化／復号化部114を備える。

再生状況分析部112は、コンテンツの再生に関する情報（例えば、コンテンツ名、再生開始日時、再生終了日時など）をコンテンツ復号部520から受信すると、これらの情報に基づいてコンテンツの再生状況を表す情報である再生状況情報（例えば、コンテンツ名に対応する再生回数、再生日、再生総時間等）を生成し、これを全体制御部113に通知する。

【0022】

全体制御部113は、コンテンツ再生条件管理部111の全体を制御する部署であり、例えばROMやRAMを備えるマイクロコンピュータである。全体制御部113は、再生状況分析部112から受信した上記再生状況情報に基づいて、暗号化／復号化部114を介して読み出したコンテンツ再生条件情報511aの更新を行い、これを暗号化してセキュアフラッシュ部120に上書きするように暗号化／復号化部114に指示する。さらに、全体制御部113は、必要に応じてTRM固有鍵格納部513に格納されているTRM固有鍵を読み出し、これを暗号化／復号化部114及びコンテンツ鍵復号部514に送信する。さらにまた、全体制御部113は、暗号化／復号化部114における暗号化処理又は復号化処理のタイミングを制御する。

【0023】

また、全体制御部113は、ICカードがカード挿入口に挿入され、新たにライセンスチケットが購入されたことを検知すると、一旦内部のRAM等に格納し、その後、このライセンスチケットをセキュアフラッシュ部120に移動（即ち、新規なライセンスチケットをセキュアフラッシュ部120に格納し、ICカード内のライセンスチケットを削除）する。

【0024】

なお、上記のように、ICカードがカード挿入口に挿入されことを検知して新たに購入されたライセンスチケットをセキュアフラッシュ部120に移動する方法に限らず、上記通信制御部（図示せず）を利用してライセンスチケットを入手し、これを全体制御部113が検知してセキュアフラッシュ部120に移動するように構成してもよい。

暗号化／復号化部114は、全体制御部113の指示に基づいて、セキュアフラッシュ部120に対するコンテンツ再生条件情報511aの読み出しと復号化処理、又は暗号化

処理と書き込みを行う。

【0025】

図3は、上記図2に示したコンテンツ再生条件管理部111における処理の流れを示すフローチャートである。

最初に、全体制御部113は、コンテンツ復号部520及び操作入力部535を介して、ユーザからコンテンツの再生指示を受け付けた旨を受信すると（S201: Yes）、当該再生指示に対応するコンテンツを特定する（S202）。

【0026】

次に、全体制御部113は、特定されたコンテンツに対応するライセンスチケットが存在する（即ち、ライセンスチケットが購入されている）か否かを確認し（S203）、確認できた場合は、上記従来の技術の場合と同様に、コンテンツ鍵を復号してコンテンツ復号部520に送信する。

上記のライセンスチケットの存否を確認する方法としては、例えば、新規に購入されたライセンスチケットをセキュアフラッシュ部120に移動する際に、当該ライセンスチケットを識別し得る情報（例えば、ライセンスチケットのID、以下「LT_ID」と略称する。）を全体制御部113内のRAMに保持しておき、上記再生指示を受け付けた際に、そのコンテンツに対応するLT_IDが全体制御部113内のRAMに存在するか否かを確認する。もし、対応するライセンスチケットが存在しない場合（S203: No）、全体制御部113は、エラー処理を実行する（S208）。

【0027】

その後、全体制御部113は、コンテンツ復号部520からコンテンツの再生に関する情報を受信すると（S204: Yes）、TRM固有鍵格納部513に格納されているTRM固有鍵を用いてセキュアフラッシュ部120に格納されているライセンスチケットを復号するように暗号化／復号化部114に指示する（S205）。

さらに、全体制御部113は、復号されたライセンスチケットのコンテンツ再生条件情報511aの内容を更新して、再び上記TRM固有鍵を用いて暗号化するように、暗号化／復号化部114に指示する（S206）。これにより、暗号化／復号化部114は、更新されたライセンスチケットを暗号化してセキュアフラッシュ部120に上書きする（S207）。

【0028】

以上のように、本実施の形態に係るコンテンツ再生装置によれば、従来TRM部（耐タンパ性を有するICカード）に格納していたライセンスチケットをセキュアフラッシュ部に格納することとしたので、TRM部における記憶容量を最小限に抑えることが可能となる。

【0029】

（実施の形態2）

上記実施の形態1においては、コンテンツに対応するライセンスチケットをセキュアフラッシュ部に格納して、TRM部の記憶容量の増大を回避する実施例について説明したが、本実施の形態では、さらに、セキュアフラッシュ部に格納されているライセンスチケットが、不正に書き換えられてしまうことを防止する実施例について説明する。

【0030】

図4は、セキュアフラッシュ部に格納されているライセンスチケットが不正に書き換えられてしまう様子を説明するための図である。図4に示されるように、例えば、あるコンテンツについては、最大「10時間」の再生を認めるようにライセンスチケットが設定されている場合に、5時間再生した場合、残りの再生可能時間は「5時間」の筈である。しかし、セキュアフラッシュ部120は、汎用のメモリであるため、任意に読出し／書き込みが可能であり、再生前の「10時間」を示すライセンスチケットのデータを他のメモリ領域に事前にコピーしておき、コンテンツを5時間再生した後に、再び「10時間」を示す古いライセンスチケットのデータを上書きすることが可能である。

【0031】

そこで、本実施の形態では、TRM部内にLT_IDとライセンスチケットのアップデート回数の対応表を保持し、この対応表に基づいて、上記の不正を防止するコンテンツ再生装置について説明する。

図5は、本実施の形態に係るコンテンツ再生装置200の機能構成を示すブロック図である。なお、本コンテンツ再生装置200においては、上記実施の形態1のコンテンツ再生装置100と同一の機能構成については同一の符番を付し、その説明は省略することとする。

【0032】

図5に示されるように、本コンテンツ再生装置200のTRM部210は、さらに、上記対応表を格納するための対応表格納部212を備える。さらにまた、コンテンツ再生装置200のコンテンツ再生条件管理部211は、対応表格納部212に格納されている対応表に基づいて、不正なライセンスチケットの上書きを防止する。

また、セキュアフラッシュ部120は、新たにLT_IDとライセンスチケットのアップデート回数との連結データに対するデジタル署名が施されたデータ221cを格納する。

【0033】

図6は、上記コンテンツ再生条件管理部211の機能構成を表すブロック図である。図6に示されるように、コンテンツ再生条件管理部211は、再生状況分析部112、全体制御部213、暗号化／復号化部114及びデジタル署名管理部214を備える。

全体制御部213は、コンテンツ再生条件管理部211の全体を制御する部署であり、例えばROMやRAMを備えるマイクロコンピュータである。全体制御部213は、上記実施の形態1における全体制御部113の機能に加え、デジタル署名管理部214の制御を行う。さらに、全体制御部213は、LT_IDとアップデート回数との組の情報（以下「連結情報」という。）を作成して保持する。

【0034】

デジタル署名管理部214は、全体制御部213の指示に基づいて、連結情報に対してデジタル署名を施してセキュアフラッシュ部120に格納すると共に、セキュアフラッシュ部120に格納されている連結情報を読み出して、その正当性を検証する。なお、上記のデジタル署名の施し方及びその検証方法は、従来の技術を使用することとする。

以下、全体制御部213が、上記対応表に基づいて古いライセンスチケットの上書きを防止する方法について、以下に示す図7を参照しながら説明する。

【0035】

図7は、対応表格納部212に格納されている対応表の一例である。図7に示されるように、対応表50には、LT_IDとアップデート回数とが対応づけられて格納されている。従って、全体制御部213が、ライセンスチケット（例えば、「ABC_0011」というライセンスチケット）についてアップデート回数をインクリメントするように管理すれば、TRM部210に保持されている連結情報と、セキュアフラッシュ部120に格納されている連結情報とを照合することによって、不正に上書きされたか否かを確認することができる。

【0036】

図8は、本実施の形態におけるコンテンツ再生条件管理部211における処理の流れを示すフローチャートである。なお、上記実施の形態1における図3のフローチャートと同一の処理については同一の符番を付し、その説明は省略する。

まず、全体制御部213は、上記実施の形態1の場合と同様に、再生指示に係るコンテンツに対応するライセンスチケットの存在を確認し（S203: Yes）、コンテンツ復号部520からコンテンツの再生に関する情報を受信すると（S206: Yes）、セキュアフラッシュ部120に格納されている、デジタル署名が施されている連結情報を読み出し、TRM固有鍵を用いて、その正当性を検証するようにデジタル署名管理部214に指示する（S601）。そして、連結情報が正当な場合（S602: Yes）、全体制御部213は、ライセンスチケットを復号するように暗号化／復号化部114に指示する（

S205)。

【0037】

さらに、全体制御部213は、コンテンツ再生条件情報511aを含むLTの内容を更新して、再び上記TRM固有鍵を用いて暗号化するように暗号化／復号化部114に指示する(S206)。さらにまた、全体制御部213は、アップデート回数をインクリメントすると共に(S603)、連結情報にデジタル署名を施すようにデジタル署名管理部214に指示する(S604)。そして、暗号化されたLT及び上記デジタル署名が施された連結情報をセキュアフラッシュ部120に書き込むように、暗号化／復号化部114及びデジタル署名管理部214に指示する(S605)。

【0038】

なお、上記の実施の形態2では、LT_IDに対応付ける情報としてアップデート回数を挙げて説明したが、アップデート回数に限らず、アップデートを行った事実を識別することが可能な乱数等の情報であってもよい。

また、上記の実施の形態2では、対応表はTRM部で保持する実施例について説明したが、対応表もセキュアフラッシュ部に格納し、対応表のハッシュ値をTRM部で保持することとしてもよい。さらにまた、ライセンスチケット毎のデジタル署名又はハッシュ値をセキュアフラッシュ部に格納し、それらのハッシュ値をTRM部で保持することとしてもよい。なお、ライセンスチケットのコンテンツ再生条件情報の中で更新する必要のない再生条件(例えば、再生可能な有効期限など)については、対応表に記載させないこととし、その分メモリ容量の軽減を図ってもよい。

【0039】

以上のように、本実施の形態におけるコンテンツ再生装置によれば、ライセンスチケットをセキュアフラッシュ部に格納すると共に、ライセンスチケットを識別し得る情報(LT_ID)とアップデート回数とが対応付けられている対応表に基づいてライセンスチケットの正当性も検証するので、TRM部の記憶容量を最小限に抑えると共に、より安全性を高めてライセンスチケットを管理することが可能となる。

【0040】

また、上記の実施の形態1及び実施の形態2では、コンテンツ復号部は、TRM部の外部に備えるように構成したが、TRM部の内部に備えることとしてもよい。

【産業上の利用可能性】

【0041】

本発明に係るライセンス情報管理装置及びライセンス情報管理方法は、著作権の保護を必要とする暗号化されたコンテンツの再生を可能とするDVD再生装置等のパッケージコンテンツの再生装置やネットワークを介して暗号化されたコンテンツを受信して再生するパーソナルコンピュータ等に利用が可能である。

【図面の簡単な説明】

【0042】

【図1】実施の形態1に係るコンテンツ再生装置の機能構成を示すブロック図である。

【図2】実施の形態1におけるコンテンツ再生条件管理部の機能構成を示すブロック図である。

【図3】実施の形態1におけるコンテンツ再生条件管理部の処理の流れを示すフローチャートである。

【図4】実施の形態1に係るコンテンツ再生装置の課題を説明するための図である。

【図5】実施の形態2に係るコンテンツ再生装置の機能構成を示すブロック図である。

【図6】実施の形態2におけるコンテンツ再生条件管理部の機能構成を示すブロック図である。

【図7】実施の形態2における対応表の一例を示す図である。

【図8】実施の形態2におけるコンテンツ再生条件管理部の処理の流れを示すフロー

チャートである。

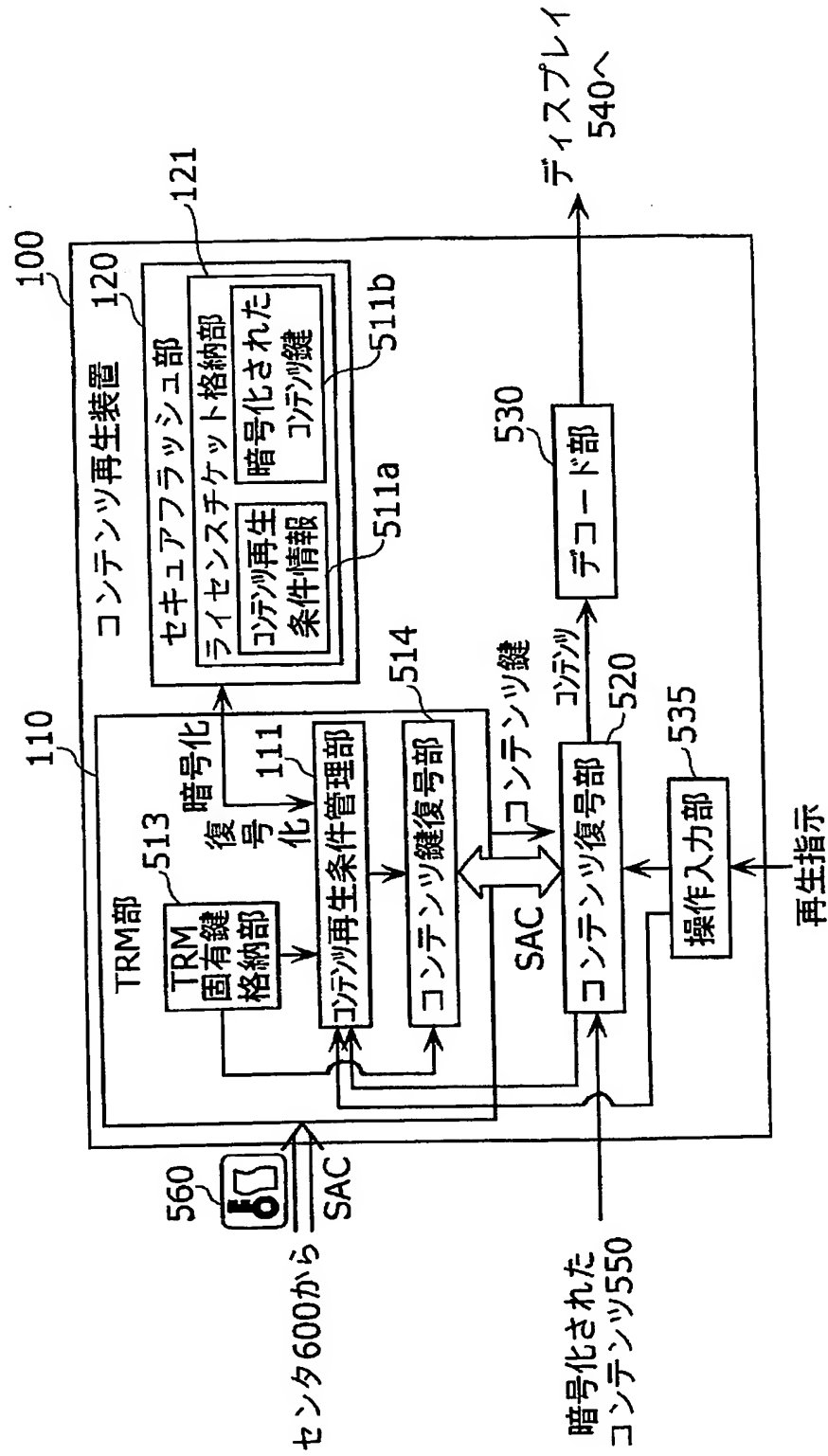
【図9】従来の技術に係るコンテンツ再生装置の機能構成を示すブロック図である。

【符号の説明】

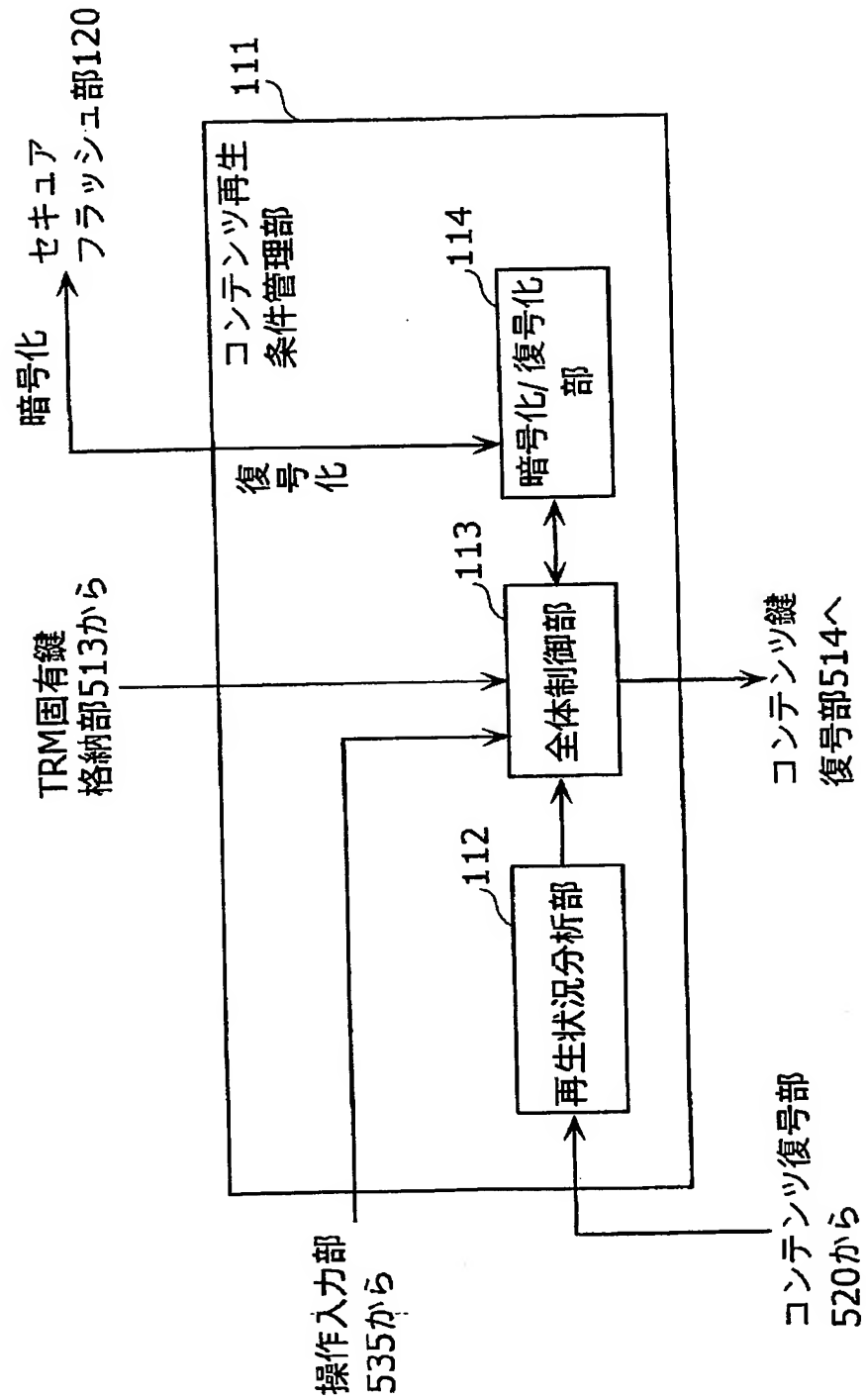
【0043】

50	対応表
100、200、500	コンテンツ再生装置
110、210、510	TRM部
111、211、512	コンテンツ再生条件管理部
112	再生状況分析部
113、213	全体制御部
114	暗号化／復号化部
120	セキュアフラッシュ部
121	ライセンスチケット格納部
212	対応表格納部
214	デジタル署名管理部
511a	コンテンツ再生条件情報
511b	暗号化されたコンテンツ鍵
513	TRM固有鍵格納部
514	コンテンツ鍵復号部
520	コンテンツ復号部
530	デコード部
535	操作入力部
540	ディスプレイ
550	暗号化されたコンテンツ
560	ライセンスチケット
600	センタ

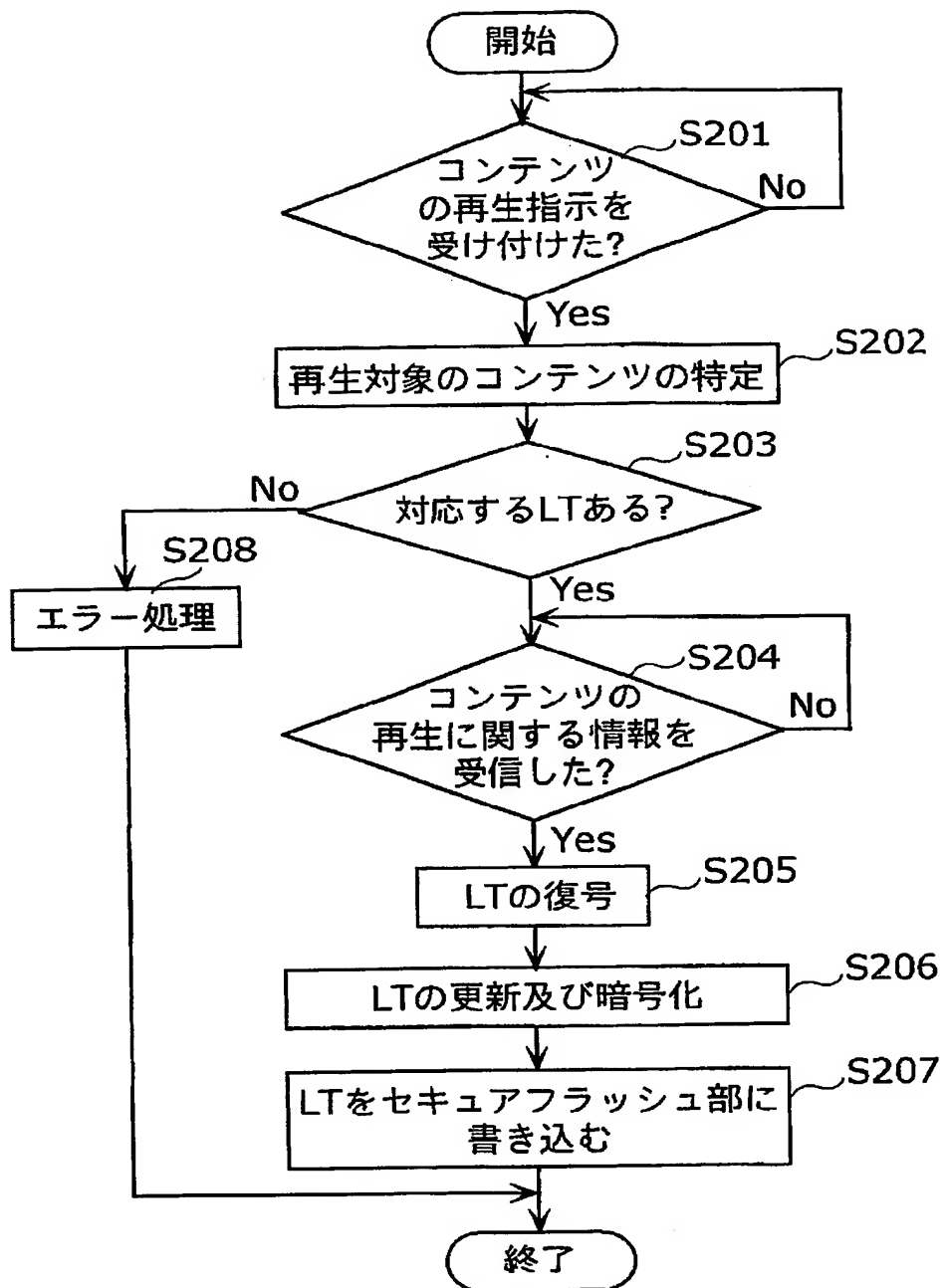
【書類名】 図面
【図1】



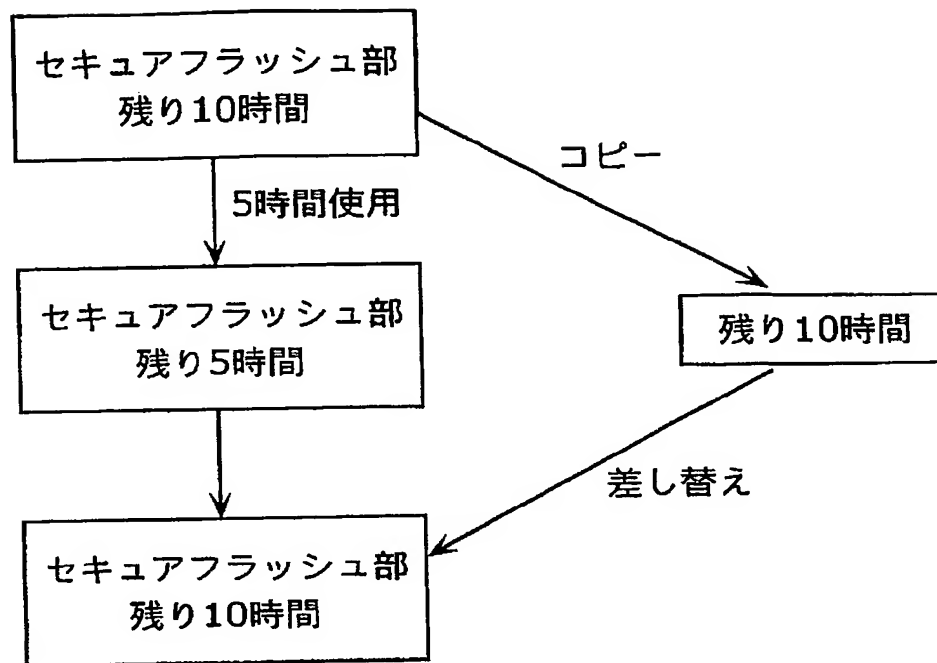
【図2】



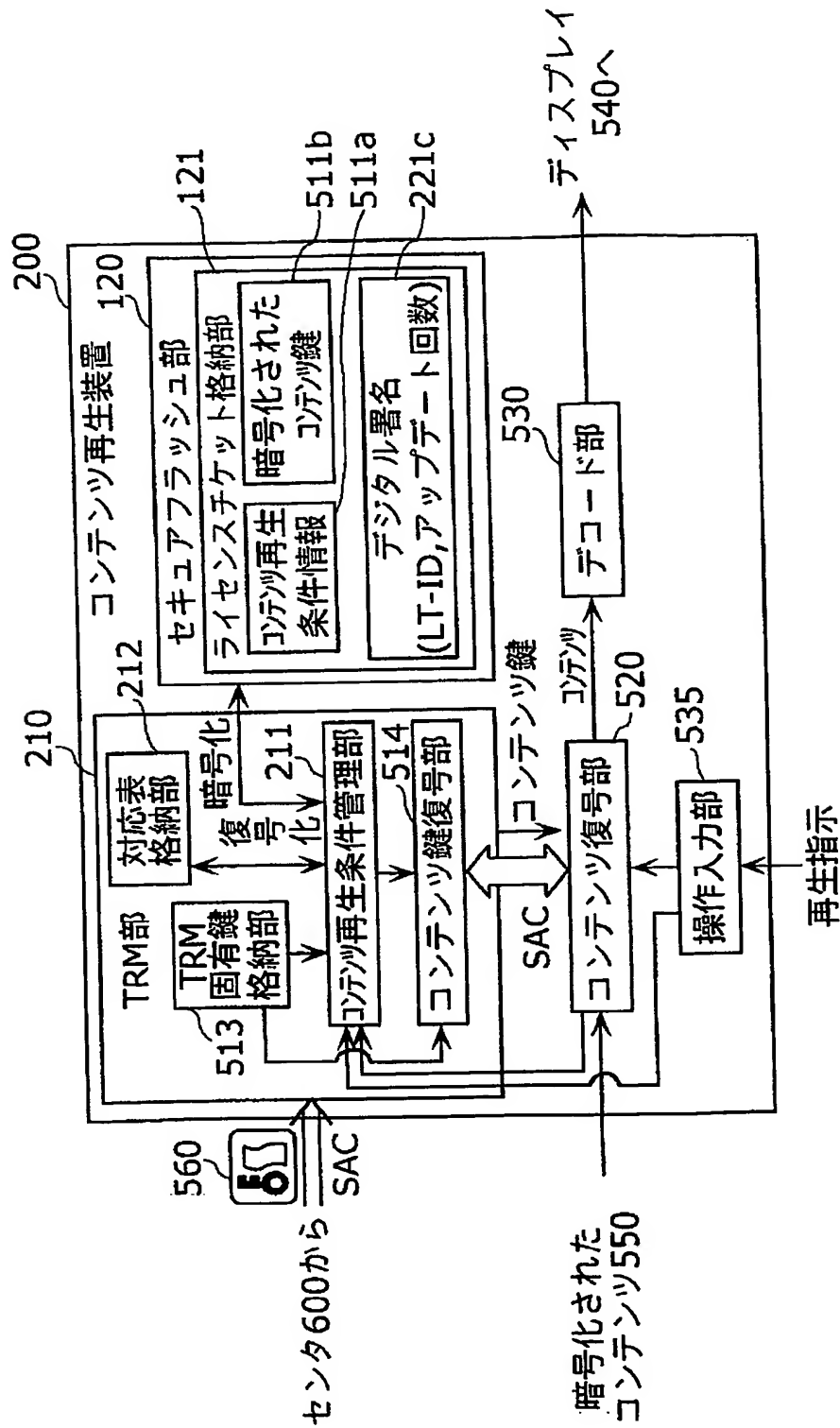
【図3】



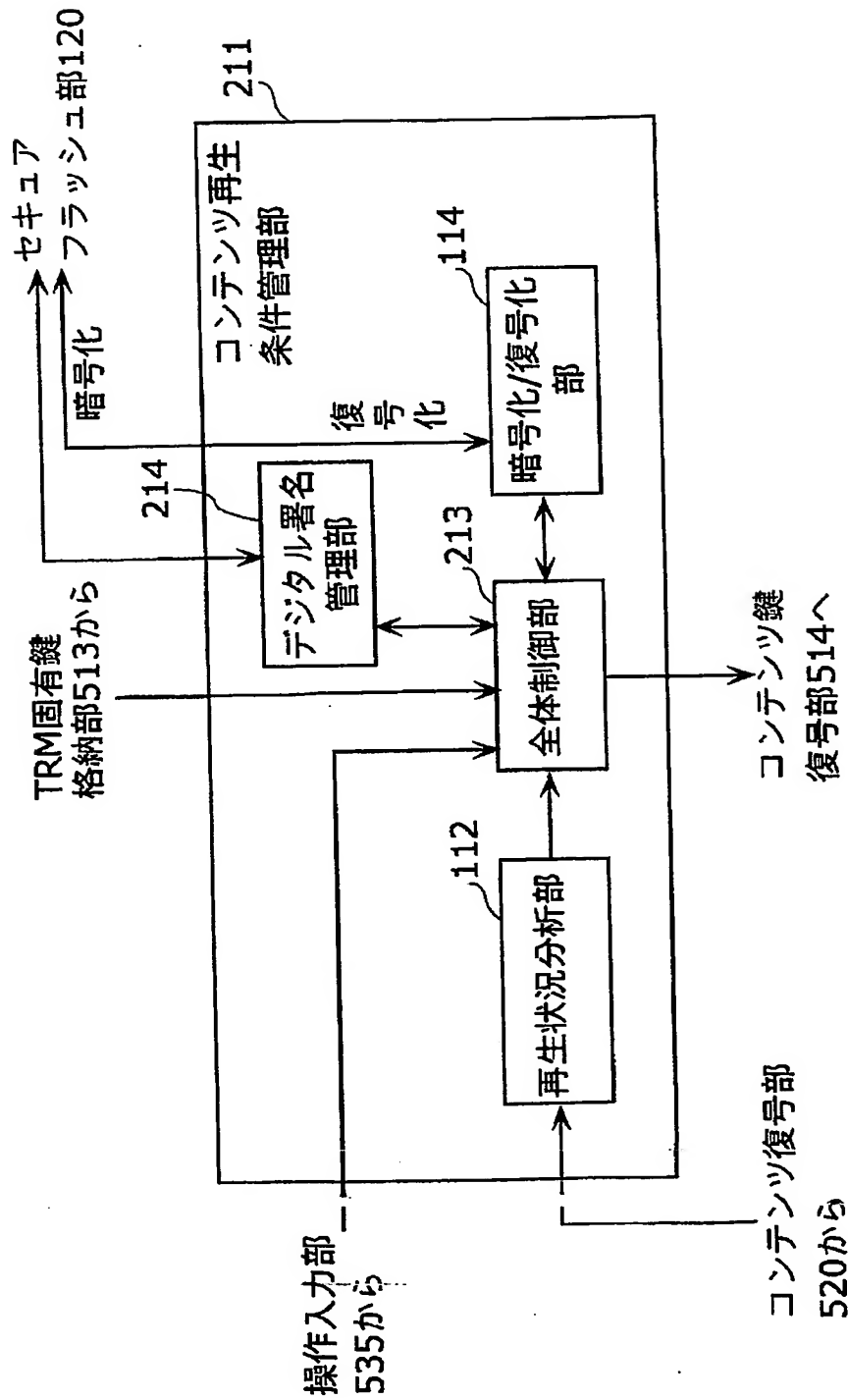
【図 4】



【図5】



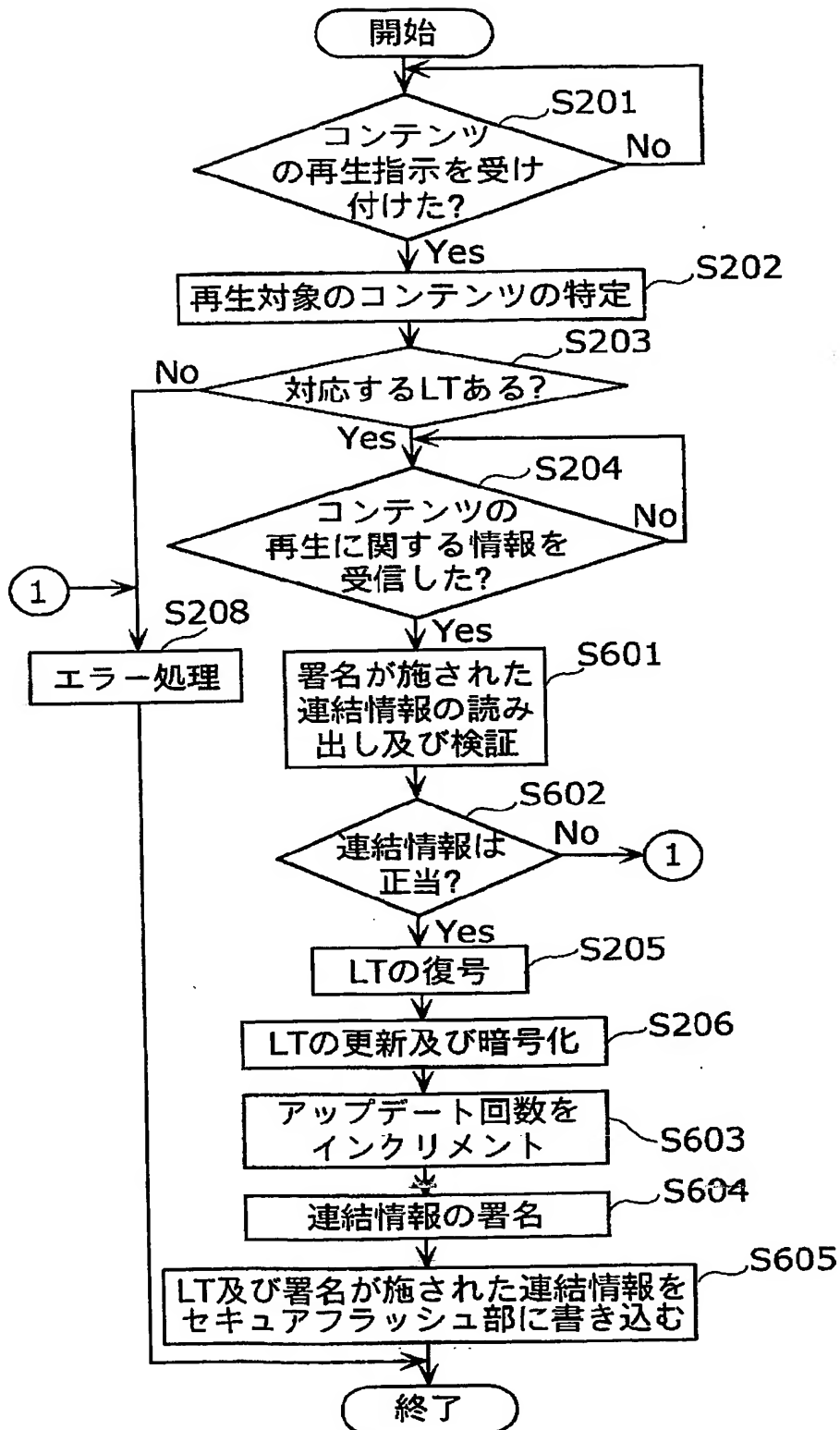
【図 6】



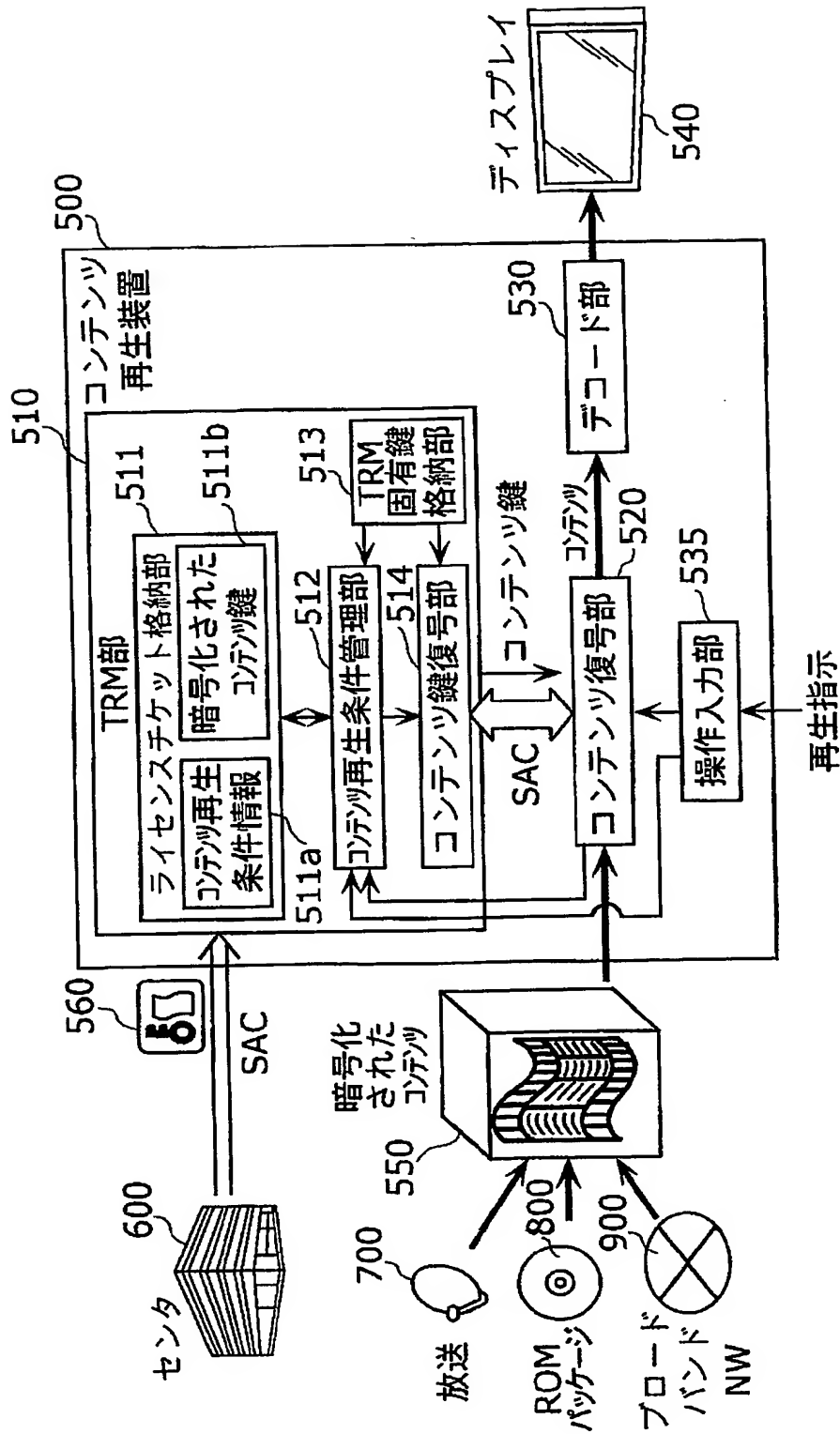
【図 7】

LT-ID	アップデート回数
ABC_0011	2
DEF_0022	5
⋮	⋮
⋮	⋮
XYZ_0099	7

【図8】



【図9】



【書類名】 要約書

【要約】

【課題】 ユーザが多数のコンテンツを所有する場合であっても、大容量の耐タンパモジュールが必要とならないライセンス情報管理装置等を提供する。

【解決手段】 全体制御部 113 は、ユーザから受信した再生指示に対応するコンテンツを特定する (S202)。全体制御部 113 は、特定されたコンテンツに対応する LT が、セキュアフラッシュ部 120 に存在するか否かを確認する。セキュアフラッシュ部 120 に LT が存在し (S203: Yes)、コンテンツ復号部 520 からコンテンツの再生に関する情報を受信すると (S204: Yes)、暗号化／復号化部 114 は、TRM 固有鍵を用いてセキュアフラッシュ部 120 に格納されている LT を復号する (S205)。その後、暗号化／復号化部 114 は、コンテンツ再生条件情報 511a の内容を更新して、TRM 固有鍵を用いて暗号化して (S207)、これをセキュアフラッシュ部 120 に書き込む (S208)。

【選択図】 図 3

認定・付加情報

特許出願の番号	特願 2004-032676
受付番号	50400211294
書類名	特許願
担当官	第七担当上席 0096
作成日	平成16年 2月10日

<認定情報・付加情報>

【提出日】 平成16年 2月 9日

特願 2 0 0 4 - 0 3 2 6 7 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002110

International filing date: 04 February 2005 (04.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-032676
Filing date: 09 February 2004 (09.02.2004)

Date of receipt at the International Bureau: 24 March 2005 (24.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse